REQUEST FOR ADDITIONAL INFORMATION 1093-7366

Issue Date: 3/24/2014

Application Title: US-APWR Design Certification - Docket Number 52-021

Operating Company: Mitsubishi Heavy Industries

Docket No. 52-021

07.07 – Control Systems

QUESTION:
07.07-34

In response to RAI No. 996-7040; Question No. 07.07-33, MHI stated in summary that MHI assumes all PCMS failures, including random hardware failures and software design defects (CCFs), are credible, and demonstrates that the US-APWR is adequately protected from the all PCMS failures and meets the DCD Chapter 15 AOO and PA acceptance criteria as follows:

1. Consequences of multiple spurious actuation signals from a single PCMS control group caused by multiple random hardware failures or a software design defect meet the DCD Chapter 15 AOO acceptance criteria.
2. Consequences of multiple spurious actuation signals of multiple non-safety components, caused by a software design defect in multiple PCMS control groups, meet the DCD Chapter 15 PA acceptance criteria.
3. Consequences of multiple spurious actuation signals of multiple safety-related and non-safety components, caused by a software design defect in one or more operational VDUs, meet the DCD Chapter 15 PA acceptance criteria.

Since the failures discussed in item 2 and 3 above are caused by software design defects, not single random hardware failures, these failures are considered as beyond design basis events. Therefore, MHI conducted these analyses using best estimate methods.

The NRC staff reviewed Sheet 1 of 5 in Table J.1-1 of the proposed changes to MUAP-07004, Appendix J to see if a single control group failure (e.g., Group 1) is bounded by the Chapter 15 AOO as described. In order to continue reviewing the RAI response, the staff needs some additional guidance related to the following :

1. **[**

]

2. **[**

]

3. **[**

]

4. **[** **]**

In addition, please provide additional design details on the Segmentation of US-APWR control functions that support the following claims:

1. The response to RAI No. 996-7040; Question No. 07.07-33 states that, "US-APWR control functions are segmented into different PCMS control groups so that a single or multiple control function failures in one PCMS control group cannot result in consequences that are more severe than the DCD Chapter 15 AOOs acceptance criteria." The RAI response also states in the attached markup of MUAP-07004-P, Revision 8, that, "Non-safety control functions are partitioned in multiple redundant PCMS controllers to limit the effects of single failures."

   a. Provide more design details on the Segmentation of US-APWR control functions. Specifically, what design attributes of the segmentation such as, diversity, independence, etc. does the applicant contend is provided by the segmentation in order to bound the effects of control group failures?

   b. Do the Control Groups shown on the PCMS FMEA under the column called "Component" on Table J.1-1 represent the segmented control functions on the PCMS controllers?

   c. Does the applicant intend to add an ITAAC to the DCD to verify the systematic allocation (segmentation) of control functions between PCMS controllers so that the PCMS FMEA is validated?

2. The applicant states in the enclosed markup of MUAP-07004-P, Revision 8, that, **[**

]

3. The PCMS FMEA, Item 20, "Operational VDU Computer Failure", references Appendix C of MUAP-07004-P. Appendix C states, in part, that **[**

]

4. Regarding Appendix J, Section J.1.1, the applicant states, in part that, for multiple functions in a single controller to be adversely affected, two random hardware failures are needed: a basic software block memory failure and a failure of the self-diagnostic circuit.

a. Clarify: Is the applicant stating that a non-safety related controller that has undergone a software fault would still be credited to detect its own failure through self-diagnostics on the same faulted controller?

b. Does the applicant intend to create an ITAAC to verify the ability of the PCMS controllers' self-diagnostic features to detect and properly respond to errors that could lead to failure of multiple functions on a single controller?

5. Appendix J, Section J.1.1, states, in part that,

"The application software of each control group is dedicatedly developed for each PCMS control group by connection and combination of the basic software blocks. Therefore, a design defect in the applicant software limits the consequences of control function failures to a single PCMS control group (i.e., it does not cause a CCF of multiple PCMS control groups)."

a. Please clarify how the application software cannot fail in such a way as to cause a software CCF on multiple control groups. The wording in this paragraph is not clear how dedicated development of each PCMS control group would sufficiently limit the effects of failure to a single control group.

b. Does the applicant mean that the application software for each PCMS control group is unique and customized specifically for each individual PCMS Control Group? If so, clarify and expound on this design aspect.